



Training Plan

Tourism Resilience Education in Digital Security



Co-funded by
the European Union

TABLE OF CONTENTS

INTRODUCTION.....	2
1.1. Purpose	2
1.2. Customisation.....	3
1.3. Delivery	3
1.4. Reference methodologies	3
1.5. EQF Levels.....	4
1.6. The framework of competencies, skills and knowledge	5
1.7. Innovative professional roles in the tourism sector related to digital security	6
TREADS TRAINING PLAN	9
2.1 Pre-requisites	10
2.2 General Learning Outcomes	10
TRAINING UNITS	12
Training Unit 1: Resilience in Tourism	12
a) Learning outcomes.....	12
b) Unit's framework and methodology.....	13
c) Sub-units.....	14
Training Unit 2: Digital Security in Tourism.....	16
a) Learning outcomes.....	16
b) Unit's framework and methodology.....	16
c) Sub-units.....	18
CONCLUSIONS.....	20

1 INTRODUCTION

The TREADS project seeks to adapt the vocational education and training (VET) offering to the challenges of the digital age. The tourism industry, deeply influenced by ICT developments and online platforms, faces the challenge of safeguarding sensitive customer data from digital and cybersecurity issues and from the proliferation of disinformation. Therefore, the project addresses issues related to ethics, privacy, confidentiality and the protection of personal data in the context of the digital transformation of the tourism industry.

In the light of these transitions, VET educators and trainers, VET students and micro-SMEs, SMEs and hospitality sector representatives as well as other travel professionals (hoteliers, tour operators, travel agents, etc.), would need to adapt with continuous training and capacity building activities to be capable of offering specialized services, dealing with disruptions and digital/cyber risks in tourism and adopting practices that enhance overall digital safety and robust mitigation measures. These efforts will also lead to better products and greater sustainability of the European tourism industry.

This document outlines the proposed TREADS Training Plan that can be adapted for students, trainers, educators, and professionals. The Training Plan focuses on the following: enhancing workforce skills to contribute to the digital transformation to drive innovative tourism development and management approaches. The Training Plan defines an updated and effective skills mix “Digitally upskilled and Resilient Tourism Expert: Conscious of Digital Risks”.

1.1. Purpose

This Training Plan was developed for VET providers, educators, students and professionals of the tourism hospitality sector to support the development and adaptation of training courses that encompasses the digital and innovative principles of the project through:

- adoption of the ECVET profile of the “Digitally Upskilled and Resilient Tourism Expert: Conscious of Digital Risks”

- adapting relevant training content for the emergent needs of the learning environment and the values they embrace

1.2. Customisation

The Training Plan is designed to create **customisable paths** at the request of specific target users by implementing and developing the areas of greatest interest and / or adapting the contents and the topics of the unit itself to specific needs and more targeted professional profiles.

Moreover, customising training content can be adjusted to accommodate the following (but not limited to):

- Specific tourism niche markets of interest
- Knowledge and technological updating
- EQF level and differing VET students: each unit can be aligned with different EQF levels, exploring the content through diverse methodological approaches according to the target

1.3. Delivery

Specifically designed for **adaptability and flexibility**, the Training Plan provides options for **classroom and online training delivery**.

The e-learning platform will, in fact, host the training courses as a distant learning resource, but will also allow for download of materials in the form of pdf documents.

Each unit is not a pre-requisite for the succeeding units. The units can be, in fact, used as a whole, but also individually depending on the objectives.

1.4. Reference methodologies

The definition of the ECVET Profile and the resulting Training Plan is based on the following methodologies:

- Strategic and systematic approach
- Customer-centric approach
- **GreenComp**, the European sustainability competence framework, which comprises four interrelated competence areas: embodying sustainability values, embracing complexity in sustainability, envisioning sustainable futures and acting for sustainability
- **DigComp**, the Digital Competence Framework for Citizens, which identifies the key components of digital competence in five areas: information and data literacy, communication and collaboration, digital content creation, safety and problem solving. In DigComp, digital competence is defined as 'the confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society'

1.5. EQF Levels

The Training Plan has been developed in accordance with the European Qualifications Framework (EQF), which consists of 8 levels that describe the learning outcomes relevant to qualifications across Europe, facilitating the recognition of skills and qualifications. Every level is defined by specific descriptors that outline the knowledge, skills and responsibilities associated with qualifications at that level¹.

The target EQF levels considered in the project are Levels 3, 4 and 5, which represent a progressive development of knowledge, skills and autonomy.

EQF Level 3, typically associated with upper secondary education, involves knowledge of facts, principles, processes and general concepts within a field of work or study. At this level, individuals are able to apply a range of cognitive and practical skills to complete tasks and solve problems by selecting and using basic methods, tools, materials and information. Learners or workers are able to complete assigned tasks and to adapt their behaviour to different circumstances, particularly when dealing with problem-solving situations.

¹ Here a detailed description of the 8 levels: <https://europass.europa.eu/en/description-eight-eqf-levels>

EQF Level 4, commonly linked to vocational education and training, is characterised by factual and theoretical knowledge in broad contexts within a field of work or study. Individuals at this level possess a range of cognitive and practical skills that enable them to generate solutions to specific problems in their professional domain. They are capable of exercising self-management within work or study contexts that are generally predictable but subject to change, and they may supervise the routine work of others, taking responsibility for the evaluation and improvement of work or learning activities.

EQF Level 5, often related to short-cycle higher education, requires comprehensive and specialised factual and theoretical knowledge within a field of work or study, together with an awareness of the boundaries of that knowledge. At this level, individuals demonstrate a broad range of cognitive and practical skills needed to develop creative solutions to abstract problems. They are able to exercise management and supervisory responsibilities in work or study contexts characterised by unpredictable change, and to review and develop both their own performance and that of others.

1.6. The framework of competencies, skills and knowledge

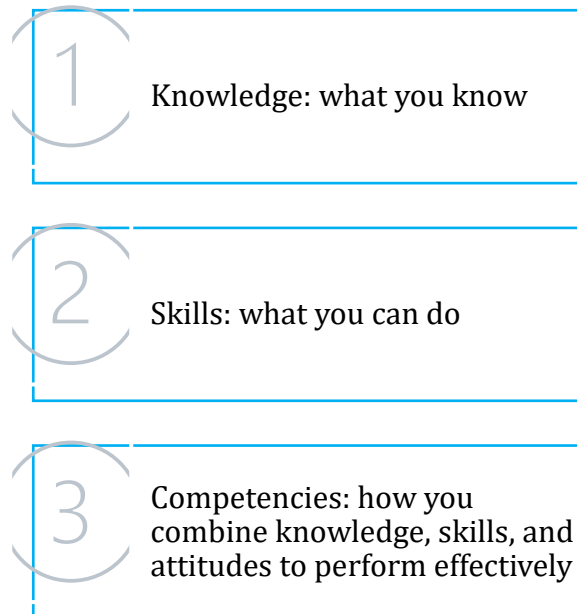
In a training plan, the framework of competencies, knowledge, and skills is essential because it provides a clear structure for learning and professional growth.

On the one hand, **knowledge** refers to the theoretical understanding of facts, concepts, principles and information related to a subject. In a training plan it's the foundation: what learners need to know in order to perform tasks effectively. On the other, **skills** are the practical abilities to apply knowledge in real situations. They involve the capacity to perform tasks, solve problems, and use tools or techniques effectively. In a training plan they are what learners must be able to do after training. They are often demonstrated through practice, exercises, or simulations. Finally, **competencies** are the integrated combination of knowledge, skills, and attitudes that enable a person to perform tasks successfully in a professional context. They represent the overall capability to act effectively and responsibly. In a training plan they are the outcomes, the objectives: what learners can achieve in complex, real-world scenarios, often requiring judgment, autonomy, and collaboration.

By combining these three dimensions, this training plan moves beyond simple information delivery and encourage holistic development, preparing learners not only to understand concepts, but also to perform tasks and take responsibility in

complex professional situations. This approach makes learning outcomes measurable, transparent, and directly aligned with workplace needs.

The key points can be summarized as follows:



1.7. Innovative professional roles in the tourism sector related to digital security

Innovative professional roles in tourism are emerging as the sector becomes increasingly exposed to digital risks. As these profiles integrate digital security, technology, user experience, and regulatory expertise and effectively address the sector's evolving needs, they are strictly linked to the new profile developed in the TREADS project.

Some examples include:

- **Digital Security Tourism Officer:** working within hotel chains, airports, DMOs, and booking platforms, this role focuses on monitoring cyber threats, managing security incidents, and training staff on phishing, social engineering, and data protection, while coordinating prevention strategies with IT and management.

- **Digital Privacy Manager for Tourism:** this professional ensures compliance with data protection regulations such as GDPR by assessing risks linked to personal and payment data, overseeing data collection in tourism CRMs, and managing clear, multilingual privacy communication for travellers.
- **Secure Travel Experience Designer:** a hybrid profile combining User Experience design, technology, and security, responsible for creating safe digital experiences such as online check-ins, smart rooms, and destination apps, integrating secure authentication, contactless systems, and risk-aware user journeys without harming usability.
- **Smart Hotel Security Specialist:** focused on automated and connected hospitality environments, this specialist secures IoT systems like smart locks and sensors, monitors internal networks, and manages vulnerabilities in building automation and energy management systems.
- **Travel Data Protection Analyst:** typically found in airlines, OTAs, and booking platforms, this role analyzes customer data flows, detects anomalies or potential breaches, and implements technical safeguards such as encryption and tokenization.
- **AI Risk & Security Specialist for Tourism:** with the rise of chatbots, facial recognition, and predictive systems, this professional evaluates ethical and security risks related to AI, prevents manipulation and model attacks, and ensures transparency and safety in AI-driven tourism services.
- **Digital Trust Manager for Tourism Destinations:** operating within DMOs and territorial organizations, this strategic role strengthens digital trust among visitors by managing cybersecurity communication, coordinating awareness campaigns, and supporting local operators on data protection issues.
- **Incident Response Coordinator for Tourism Facilities:** an operational role activated during cyberattacks or data breaches, responsible for coordinating technical teams and external providers, managing crisis communication, restoring systems, and conducting post-incident analysis.

These profiles will have the opportunity to work across a wide-range of tourism-sector organizations including hospitality and accommodation providers (hotels, camping villages, serviced apartments); transport and mobility operators (airlines, cruise companies, rail companies, car rental and mobility-as-a-service platforms);

online travel and booking platforms (OTAs, metasearch engines, tour operator digital platforms, dynamic packaging systems); destination management and territorial organizations (DMOs, regional and municipal tourism boards, visitor centres and tourism promotion agencies); cultural, natural and recreational attractions (museums, archeological sites, heritage centres, entertainment venues, protected natural areas and national parks, smart-tourism attractions using IoT and digital ticketing); tour operators and travel agencies (traditional travel agencies, tour operators, niche and experiential travel companies, corporate travel management firms); technology providers for tourism (companies developing hotel PMS, CRS, CRM systems, IoT providers for smart rooms and building automation, cybersecurity firms specializing in tourism, AI solution providers such as chatbots, facial recognition, predictive analytics); and large tourism facilities and integrated resorts (convention centres, casinos and entertainment complexes, integrated resorts with hotels, malls and attractions).

The goal of the TREADS training plan to define an updated and effective skills mix of the “Digitally upskilled and Resilient Tourism Expert: Conscious of Digital Risks” is adaptable to the evolving needs of the tourism sector; it is, moreover, grounded on the EU principles and framework of sustainability and digital transition and in line with the European Data Strategy, the EU Green Deal and the Pact for Skills.

The digitally upskilled and resilient tourism expert will be able to create ethical data practices, digital security strategies, and contingency plans that go beyond post-attack investigations or compliance obligations. Therefore, this expert is envisioned to be at the forefront of promoting and leading a more responsible workforce toward a more resilient and secure tourism sector, aware of digital threats and how to manage them.

This document describes the critical components of the training course along with its associated training outputs and assessment criteria. Additionally, this document, which refers to the ECVET Profile, outlines the knowledge, skills, and competences necessary for developing and promoting digitally safe tourism environments, aiming to foster resilient and sustainable tourism professionals and to enhance awareness of current cybersecurity challenges within the tourism industry.

This Training Plan is structured into two main training units, each composed of three sub-units, for a total duration of 96 hours (48 hours of training per unit). The modular design of the course allows for a high degree of flexibility: the units may be delivered as a complete and integrated learning pathway, or they may also be implemented individually or selectively, depending on the specific learning objectives, target groups, or training contexts.

The Training Plan has been developed in accordance with the European Qualifications Framework (EQF) at **Level 4**, ensuring that learners acquire practical and operational competences applicable in real working environments. At the same time, the structure and learning outcomes are designed to be **adaptable to EQF Level 5** for more advanced or specialized target groups, as well as **partially usable at EQF Level 3 for introductory or foundational training purposes**. This flexibility enhances the transferability and scalability of the training across different vocational education and training (VET) contexts and learner profiles.

Regarding the allocation of ECVET points to the two units composing the Training Plan, there is no single definition, as the allocation depends on the weight of the units within qualification pathways and on the **complexity, scope, and volume of learning outcomes in each unit**. Based on the general guideline assigning 60 points to a full year of VET, an estimate of **0.06 ECVET points per hour** can be made, resulting in a **total of 5.76 points** (2.88 points per unit). However, as mentioned, this is only an indicative estimate and is not binding.

2.1 Pre-requisites

Participants are expected to possess basic technical knowledge related to the tourism sector, including an introductory understanding of tourism technologies, tourist routes and products, relevant tourism legislation, as well as basic principles of accounting and administrative procedures. In addition, learners should have basic digital competences at European level, enabling them to use standard computer tools and online platforms effectively.

A minimum language competence at B1 level (according to the Common European Framework of Reference for Languages) is recommended to ensure learners can follow training materials, participate in collaborative activities, and engage with case studies and simulations, particularly in an international or European context.

Beyond formal prerequisites, the Training Plan is intended for learners who demonstrate motivation and professional interest in developing skills related to resilience, digital transformation, and digital security within the tourism sector.

2.2 General Learning Outcomes

Upon completion of the training, participants are expected to achieve a set of concrete and measurable learning outcomes. These include the acquisition of objective and job-relevant skills, directly applicable to tourism organisations and destinations. The learning process emphasizes a strong practical orientation, supported by application workshops, hands-on exercises, and real-life simulations that reflect authentic professional scenarios.

Learners will also be involved in project-based work, encouraging problem-solving, teamwork, and the integration of knowledge across different thematic areas. The successful completion of the Training Plan is subject to the successful completion of

Training Plan

the assessments, designed to evaluate both theoretical understanding and practical competencies. Participants who meet the assessment criteria will demonstrate their readiness to apply resilience and digital security principles effectively within the tourism sector.



Training Unit 1: Resilience in Tourism

a) Learning outcomes

Knowledge

By the end of the training, the learner will be able to explain the key concepts of organizational and community resilience and understand their relevance to the tourism sector. They will be able to identify major risk and vulnerability factors that can affect tourism activities, including health, climate, geopolitical, and digital risks. The learner will also be able to describe the relationship between resilience and the ongoing green and digital transitions in tourism, and recognize relevant European policy frameworks, such as the Sustainable Development Goals (SDGs), the EU Green Deal, and the EU Digital Strategy. Furthermore, they will understand the basic principles of crisis management and post-crisis recovery within tourism organizations.

Skills

The learner will be capable of identifying and assessing risks and vulnerabilities in a tourism business or destination. They will be able to contribute to the development of basic resilience and crisis response plans, applying sustainability and digitalization principles to strengthen tourism resilience. In addition, learners will participate effectively in crisis simulations and role-play activities, and support recovery strategies following a crisis scenario in a tourism context.

Competencies

The learner will demonstrate a degree of autonomy when performing routine resilience-related tasks, following established procedures. They will cooperate with colleagues and other stakeholders during crisis situations and take responsibility for implementing resilience measures within their role in a tourism organization.

b) Unit's framework and methodology

DURATION

48 hours (16 for each subunit)

METHODS OF DELIVERY

The unit can be delivered online, through individual or group-based learning, or in person.

PRACTICAL ACTIVITIES AND RELATED OUTPUTS

- Analysis of real cases of resilient destinations, followed by the drafting of a report
- Group workshop: design of resilience plans tailored to different destinations leading to the drafting of a comprehensive Tourism Resilience Plan and to a group presentation before the trainer and the other students
- Role-playing activity: simulating a hotel management committee's decision-making process during a crisis, followed by the drafting of a debriefing report
- The practical activities may be carried out individually or in groups, depending on the context.

ASSESSMENT

- Online quizzes on European frameworks and SDGs
- Evaluation of the practical activities through, for example, questionnaires, quizzes, hackatons, reports, group presentations

The learner's performance will be assessed through their ability to correctly identify and classify risks in a given tourism case study and to demonstrate appropriate decision-making during simulated crisis scenarios. They will contribute to the preparation of written or oral resilience action plans for tourism organizations and actively participate in role-play and group activities, showing problem-solving skills and teamwork. In addition, learners will be expected to complete knowledge-based tests or quizzes with satisfactory results.

c) Sub-units

SUB-UNIT 1: INTRODUCTION TO RESILIENCE

At the end of this sub-unit, learners will be able to identify vulnerabilities in a tourism business or destination, assess risk probability and impact, recognize signals of potential crises and communicate risks to non-technical stakeholders.

- Types of resilience (organizational resilience, community resilience, destination resilience) and their relevance to the tourism sector
- Human factor in resilience (staff adaptability, leadership, teamwork, mental well-being)
- Risk and vulnerability factors in tourism (for example, natural disasters, pandemics, geopolitical instability, digital threats)
- Early warning systems (indicators and signals of crisis escalation)

Suggested practical activity:

- Risk mapping exercise for a small hotel or travel agency

SUB-UNIT 2: RESILIENCE AND TWIN TRANSITIONS (GREEN & DIGITAL)

At the end of this sub-unit, students will be able to apply SDGs to tourism operations, identify green and digital synergies, evaluate smart solutions for resilience improvement and collaborate with public authorities and tech providers.

- Climate change impact on tourism (heatwaves, water scarcity, seasonality shifts)
- Integration of UN Sustainable Development Goals (SDGs) and circular economy principles into tourism models.
- Smart technologies in tourism (Smart Tourism Destinations, IoT sensor – energy, water, occupancy, AI for demand forecasting and crisis response)
- European framework: EU Green Deal, EU Digital Strategy and inclusion.

Suggested practical activity:

- Case analysis of a smart tourism destination in Europe

SUB-UNIT 3: RESILIENCE PLANNING IN TOURISM

At the end of this sub-unit, learners will be able to contribute to a basic crisis response plan, participate in crisis decision-making processes and prioritize actions under pressure.

- Crisis lifecycle: prevention, preparedness, response, recovery, learning
- Focus on:
 - post-crisis recovery strategies for tourism businesses
 - reputation and trust recovery (online reviews, media relations, customer communication)
 - after-action reviews and continuous improvement
- Crisis management in three areas: health, climate and digital.

Suggested practical activity:

- Role-play: simulating a management committee responding to a crisis in a tourism business, such as a hotel.

Training Unit 2: Digital Security in Tourism

a) Learning outcomes

Knowledge

By the end of the training, the learner will be able to describe basic digital security concepts and understand the most common digital threats affecting the tourism sector. They will recognize typical vulnerabilities in digital tourism processes, such as online reservation systems, digital payments, and data management practices. The learner will also understand fundamental principles of digital security, including the concept of Zero Trust Security, and will be able to identify basic regulatory requirements related to data protection and digital security, such as the General Data Protection Regulation (GDPR). In addition, they will understand how digital incidents can affect business continuity and the reputation of tourism organizations.

Skills

The learner will be able to apply basic digital security practices in daily tourism operations and follow secure procedures when handling customer data, online bookings, and digital payment systems. They will be capable of detecting and reporting suspicious digital activities, such as phishing attempts or online fraud, and of responding appropriately to simulated cyber incidents, including data breaches or ransomware attacks. Furthermore, learners will be able to contribute to internal communication and response procedures during digital crises.

Competencies

The learner will work responsibly with digital systems and customer data in accordance with established security policies. They will support organizational responses to digital security incidents within their level of responsibility and will be able to adapt their behavior and procedures in order to reduce digital risks in tourism environments.

b) Unit's framework and methodology

DURATION

48 hours (16 for each subunit)

METHODS OF DELIVERY

The unit can be delivered online, through individual or group-based learning, or in person.

PRACTICAL ACTIVITIES AND RELATED OUTPUTS

- Basic security assessment of a tourism-related website identifying potential vulnerabilities related to data protection, online bookings, and user access. A short security audit report outlining identified risks and recommended mitigation measures will be prepared afterwards
- Case study on a ransomware attack on a hotel Property Management System (PMS). Learners will analyze a realistic case study focusing on causes, impacts and response actions and will write a case analysis describing the incident, the response strategy and the lessons learned
- Workshop on communication planning for data leak crises: through group work, learners design and draft a communication plan addressing internal and external communication during a data leak or digital security incident and present their work to the trainer and to the other students
- Simulated phishing attacks and online reservation fraud scenarios, followed by a checklist documenting correct responses and improvement areas
- Development of a comprehensive digital security plan for a tourism agency or hotel, including preventive measures, response procedures and roles

The practical activities may be carried out individually or in groups, depending on the context.

ASSESSMENT

- Short quizzes on theoretical knowledge
- Evaluation of the practical activities through, for example, questionnaires, quizzes, hackatons, reports, checklists, group presentations

The learner's achievement will be assessed through their ability to correctly identify digital security risks in practical, tourism-related scenarios. They will be expected to demonstrate the secure use of digital tools during simulations or hands-on exercises, as well as successfully complete phishing or fraud detection simulations. Assessment will also consider the learner's contribution to the development of a

basic digital incident response or communication plan. Finally, learners must pass final assessments that combine theoretical knowledge with practical application.

c) Sub-units

SUB-UNIT 1: FUNDAMENTALS OF DIGITAL SECURITY

At the end of the sub-unit, learners will be able to recognize unsafe digital behavior, apply basic security rules in daily work, report incidents correctly, and understand roles and responsibilities.

- Basic concepts of digital security
 - Cyber hygiene (password management, MFA, updates, backups)
 - Human factor in digital security
 - Regulatory framework (GDPR basics for tourism staff), NIS2 Directive (overview, relevance for tourism supply chain)
- Most common digital threats in the tourism sector
- Disinformation and social engineering targeting tourism businesses (fake reviews, false alerts, manipulated customer communications)
- Introduction to Zero Trust Security

Suggested practical activity:

- Digital security awareness quiz

SUB-UNIT 2: SECURITY IN DIGITAL TOURISM PROCESSES

At the end of this sub-unit, students will be able to follow secure procedures for bookings and payments, handle customer data responsibly, act correctly during a suspected data breach, collaborate with IT and security teams.

- Secure customer data management: protection of online reservations and payments
- Blockchain for payments and beyond payments (traceability, identity verification, loyalty programs)

- Response protocols for data breaches (roles and responsibilities in the first 24 hours)

Suggested practical activity:

- Scenario-based exercise: suspicious payment activity

SUB-UNIT 3: SIMULATIONS AND DIGITAL CRISIS MANAGEMENT

At the end of this sub-unit, students will be able to react correctly in digital emergencies, communicate clearly and responsibly, avoid escalation of damage and support recovery actions.

- Types of cyber incidents: phishing and reservation fraud, ransomware, DDoS, data leaks, account takeovers
- Communication hierarchy: internal staff, customers, authorities (DPA), media
- Post incident recovery: system restoration and trust rebuilding
- Psychological pressure during digital crisis

Suggested practical activity:

- Case study: ransomware attack on a hotel PMS.
- Workshop: communication plan for data leak crises.

The TREADS training course aims at equipping VET trainers and educators, students and professionals from the tourism sector with the necessary competencies and skills to face emerging digital threats and sustainability challenges, in order to foster the digital and sustainable transformation of the tourism industry. If the tourism industry wants to remain competitive, trustworthy, and secure in the digital era, training its professionals in resilience and digital security becomes paramount.

The TREADS Training Plan, designed in accordance with the EU Green Deal and the Pact for Skills, describes the key components of the training course for the profile “Digitally Upskilled and Resilient Tourism Expert: Conscious of Digital Risks,” including the course structure and unit breakdown, learning outcomes, prerequisites, delivery, suggested practical activities and assessment methodology.

This Training Plan allows the creation of workplace or vocational training courses for different types of users, offering flexibility in the selection of lessons.

To make the course adaptable to the training needs of each trainer and trainee, in fact, the concept of lean and micro-learning is applied to the course structure, with short-form, stand-alone units of study.

Additionally, TREADS training is transferable for use to all EU countries due to the implementation of the ECVET Framework, which is based on competencies, skills and knowledge. Its structure approach is therefore applicable to Tourism VET programs in all EU countries.



 treadsproject.eu

 [treads-project](https://www.linkedin.com/company/treads-project)

 [Treads Project](https://www.facebook.com/TreadsProject)

 [treadsprojecteu](https://www.instagram.com/treadsprojecteu)



Co-funded by the
European Union

Co-funded by the European Union. The opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the Spanish Service for the Internationalization of Education (SEPIE). Neither the European Union nor the granting authority can be held responsible for them